Proprietary Software Is Often Malware

Table of contents Latest additions

Proprietary software, also called nonfree software, means software that doesn't respect users' freedom and community. A proprietary program puts its developer or owner in a position of power over its users. This power is in itself an injustice.

The point of this directory is to show by examples that the initial injustice of proprietary software often leads to further injustices: malicious functionalities.

Power corrupts; the proprietary program's developer is tempted to design the program to mistreat its users. (Software designed to function in a way that mistreats the user is called malware.) Of course, the developer usually does not do this out of malice, but rather to profit more at the users' expense. That does not make it any less nasty or more legitimate.

Yielding to that temptation has become ever more frequent; nowadays it is standard practice. Modern proprietary software is typically an opportunity to be tricked, harmed, bullied or swindled.

Online services are not released software, but in regard to all the bad aspects, using a service is equivalent to using a copy of released software. In particular, a service can be designed to mistreat the user, and many services do that. However, we do not list instances of malicious dis-services here, for two reasons. First, a service (whether malicious or not) is not a program that one could install a copy of, and there is no way at all for users to change it. Second, it is so obvious that a service can mistreat users if the owner wishes that we hardly need to prove it.

However, most online services require the user to run a nonfree app. The app is released software, so we do list malicious functionalities of these apps. Mistreatment by the service itself is imposed by use of the app, so sometimes we mention those mistreatments too—but we try to state explicitly what is done by the app and what is done by the dis-service.

When a web site provides access to a service, it very likely sends nonfree JavaScript software to execute in the user's browser. Such JavaScript code is released software, and it's morally equivalent to other nonfree apps. If it does malicious things, we want to mention them here.

When talking about mobile phones, we do list one other malicious characteristic, location tracking which is caused by the underlying radio system rather than by the specific software in them.

As of December 2023, the pages in this directory list around 600 instances of malicious functionalities (with more than 710 references to back them up), but there are surely thousands more we don't know about.

Ideally we would list every instance. If you come across an instance which we do not list, please write to webmasters@gnu.org to tell us about it. Please include a reference to a reputable article that describes the malicious behavior clearly; we won't list an item without documentation to point to.

If you want to be notified when we add new items or make other changes, subscribe to the mailing list <www-malware-commits@gnu.org>.

Injustices or techniques	Products or companies
Addictions Back doors (1) Censorship Coercion Coverups Deception DRM (2) Fraud Incompatibility Insecurity Interference Jails (3) Manipulation Obsolescence Sabotage Subscriptions Surveillance Tethers (4) Tyrants (5) In the pipe	Appliances Cars Conferencing EdTech Games Mobiles Webpages Adobe Amazon Apple Google Microsoft

1. *Back door:* any feature of a program that enables someone who is not supposed to be in control of the computer where it is installed to send it commands.
2. *Digital restrictions management, or "DRM":* functionalities designed to restrict what users can do with the data in their computers.
3. *Jail:* system that imposes censorship on application programs.
4. *Tether:* functionality that requires permanent (or very frequent) connection to a server.
5. *Tyrant:* system that rejects any operating system not "authorized" by the manufacturer.

Users of proprietary software are defenseless against these forms of mistreatment. The way to avoid them is by insisting on free (freedom-respecting) software. Since free software is controlled by its users, they have a pretty good defense against malicious software functionality.

Latest additions

2024-01

UHD Blu-ray denies your freedom — The anatomy of an Authoritarian Subjugation System

2022-07

UEFI makes computers vulnerable to advanced persistent threats that are almost impossible to detect once installed...

- 2024-05

  Spotify sold a music streaming device but they no longer support it. Due to its proprietary nature, it can no longer be updated or even used. Users requested Spotify to make the software that runs on the device libre, and Spotify refused, so these devices are now e-waste. Spotify is now offering refunds to save the purchasers from losing money on these products, but this wouldn't prevent the products from being e-waste, and wouldn't save users from being jerked around by Spotify. This is an example of how software that is not free controls the user instead of the user controlling the software. It is also an important lesson for us to insist the software in a device be libre before we buy it.

- 2024-03

  Microsoft is using malware tactics to get users to switch to their web browser, Microsoft Edge, and their search engine, Microsoft Bing. When users launch the Google Chrome browser Microsoft injects a pop up advertisement in the corner of the screen advising users to switch to Bing. Microsoft also imported users Chrome browsing data without their knowledge or consent.

- 2024-03

  GM is spying on drivers who own or rent their cars, and give away detailed driving data to insurance companies through data brokers. These companies then analyze the data, and hike up insurance prices if they think the data denotes “risky driving.” For the car to make this data available to anyone but the owner or renter of the car should be a crime. If the car is owned by a rental company, that company should not have access to it either.

- 2023-12

  Surveillance cameras put in by government A to surveil for it may be surveilling for government B as well. That's because A put in a product made by B with nonfree software.

  (Please note that this article misuses the word “hack” to mean “break security.”)

- 2023-11

  Microsoft has been annoying people who wanted to close the proprietary program OneDrive on their computers, forcing them to give the reason why they were closing it. This prompt was removed after public pressure.

  This is a reminder that angry users still have the power to make developers of proprietary software remove small annoyances. Don't count on public outcry to make them remove more profitable malware, though. Run away from proprietary software!

More items...